HWG | HARRIS, WILTSHIRE & GRANNIS LLP

1919 M STREET NW
SUITE 800
WASHINGTON DC 20036

TEL +1 202 730 1300
FAX +1 202 730 1301
HWGLAW.COM

ATTORNEYS AT LAW

December 22, 2017

VIA ECFS

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: *Structure and Practices of the Video Relay Service Program*, CG Docket No. 10-51; *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, CG Docket No. 03-123

Dear Ms. Dortch:

Sorenson Communications, LLC ("Sorenson") writes to reply to Neustar's *ex parte* letter dated December 13, 2017,[1] which responds to the concerns Sorenson raised about requiring deaf users of public videophones to log in using the OAuth protocol. As Sorenson explained in its prior filing, there is no good reason to require users to log in before placing calls from a public phone because there is virtually no risk that public phones would be used to place ineligible calls. Neustar does not dispute this and "takes no position on the merits of whether such logins for public videophones should be required." Neustar also does not dispute that requiring users to memorize login information or to carry a smartphone in order to make a call would place a unique burden on deaf individuals that is not functionally equivalent.

Nor does Neustar seriously challenge the issues that Sorenson raised with OAuth in particular. Instead, Neustar obfuscates and misleads, suggesting that it is a simple matter to add a browser. This is simply not correct. In further misdirection, Neustar invokes software-based VRS endpoints—examples of which would be smartphones, tablets, and laptops. Of course, if a VRS user had these and access to WiFi or a CMRS network, they would not need a public phone. With significant implementation costs, lack of any discernible benefit in preventing waste, fraud or abuse, and making VRS less functionally equivalent to hearing telephone service, it is apparent that the only beneficiary of Neustar's proposal is Neustar.

---

[1] *See* Letter from Richard L. Fruchterman, III, Sr. External Affairs Counsel, Neustar, to Marlene H. Dortch, Secretary, FCC, CG Docket Nos. 10-51 and 03-123 (dated Dec. 13, 2017) ("*Neustar Letter*").

1. Adding a Custom-Browser to the Majority of Public VRS Phones is Costly and Compromises Network Security

Neustar concedes that if the Commission requires providers to implement OAuth, "VRS devices that do not have a web browser, or are not upgraded to have a minimal web browser, could not be used as public VRS devices."[2] As Sorenson explained in its prior filing, this would make inoperable all of the nearly 3,000 nTouch VP1 or VP2 public phones that Sorenson has installed at the request of schools, government agencies, healthcare providers, and many other public and private intuitions that provide services to the deaf. These devices do not contain a keyboard or a system web browser. Neustar blithely dismisses this concern and suggests that Sorenson must be confused about the costs of implementing OAuth because a "public VRS device needs only a simple web browser." But modifying the nTouch VP1 or VP2 to accommodate a web browser is no simple task: although Sorenson could modify these devices to run a custom-written browser, doing so would be prohibitively expensive and would make the devices less secure. It would also be contrary to the security standards outlined in the OAuth protocol, which calls for the use of a system browser.[3] Any browser added by Sorenson to its embedded platforms, if it is even possible, would be a browser using a mix of open source and custom code and would be developed at considerable cost.

Adding browser and login capability would also create additional security challenges. Sorenson's nTouch VP1 and VP2 videophones were intentionally designed not to have a keyboard or a browser, which enhances security and makes it more difficult to tamper with the device. Because of the lack of a keyboard, users would have to log in using a remote control and an on-screen keyboard, making their credentials vulnerable to theft by anyone nearby. Moreover, it would not be surprising if users shared credentials or even posted credentials next to public videophones, a practice that would be virtually impossible to police and which would render the login requirement meaningless.

2. Software-Based Endpoints—A Small Minority—Do Not Show that OAuth is Appropriate for Fixed-Point Public Phones.

Neustar also notes that providers offer software-based endpoints, which do have web-browser capability. But Neustar fails to acknowledge that the vast majority of public phones are not software-based endpoints. All of Sorenson's public phones (which are presumably the vast majority of public phones in the market given Sorenson's share of VRS subscribers) are nTouch

---

2 *Neustar Letter* at 1.

3 OAuth 2.0 Threat Model and Security Considerations states, in part:

> Client developers should not write client applications that collect authentication information directly from users and should instead delegate this task to a trusted system component, e.g., the system browser.

See RFC 6819 OAuth 2.0 Threat Model and Security Considerations (Jan. 2013) at 20 *available at* https://www.rfc-editor.org/rfc/pdfrfc/rfc6819.txt.pdf

VP1s or VP2s—not software-based endpoints. The predominant use of software-based endpoints today is for use with mobile devices—whether smartphones, tablets or laptops. Of course, if a VRS use has one of these, and has access to a CMRS network (as all smartphones do) or a WiFi network (as is common in airports, coffee shops, and educational institutions, among many other places), a VRS user would not need to use a public phone. They could simply use their mobile VRS, just as hearing users use mobile phones rather than pay phones.

Replacing thousands of nTouch devices with software-based endpoints would cost at least $2 to $3 million (not including the costs of modifying the software to permit log in). And doing so would also be a technological step backwards for VRS consumers. Sorenson's nTouch devices are its flagship product. Institutions have chosen almost exclusively to use Sorenson's videophones as their public devices precisely because of the innovative design and ease of use for Deaf communication. In many locations, Sorenson's videophones are custom built into phone booth kiosks. Retrofitting these kiosks to use PC or MAC computers may not even be possible, and surely would be less reliable and harder to maintain than today's purpose built VP1 and VP2 devices. Requiring institutions to give up these devices in favor of software-based products would undermine consumer choice.

Even more troubling for the industry is Neustar's disclosure that even if an iTRS provider does not provide public devices, it nevertheless will be required to create a central OAuth server to authenticate their users when invoked by the Neustar OAuth proxy. Rather than attempting to calculate the cost of this add-on requirement to a provider, Neustar simply notes that providers that do not have such capability would need to develop it. Even if the cost to implement OAuth servers and username/password capability would be modest for some providers, forcing all providers to implement such capability is nonsensical given the absence of any evidence that it is necessary.

3. A Login Requirement for Public VRS Phones Using OAuth or Otherwise Violates the Paperwork Reduction Act.

Finally, forcing users to log in before placing calls and requiring any Deaf user that may have a future requirement to use a public VRS phone to carry or have memorized some form of credential, on the chance they would be in a situation that required the use of a videophone located in public spaces or in businesses, would represent a "collection of information" within the meaning of the Paperwork Reduction Act ("PRA"), 44 U.S.C. 3501 *et seq*., as more than ten people or entities would be required to provide information to a third party (the VRS provider). As Sorenson has already explained in its previous letter, there is no demonstrable waste, fraud, or abuse of VRS by ineligible individuals using a public phone: an ASL-speaking hearing person is extremely unlikely to use VRS to communicate with another hearing person, which is the only conceivable form of waste, fraud, or abuse that a login requirement would address.[4] Collection

---

[4] *See* Letter from John T. Nakahata, Counsel to Sorenson Communications, LLC, to Marlene H. Dortch, Secretary, FCC, at 2, CG Docket Nos. 10-51 and 03-123 (dated Nov. 30, 2017).

of this information for calls from public videophones also exposes consumers to risks of identify theft and raises information security concerns, as explained above. With no benefits of waste, fraud, or abuse prevention, a login requirement could not possibly pass the PRA's requirement for agencies to balance the costs of information collections against the benefits. As discussed above, a login requirement, especially using OAuth as Neustar proposes, is exceptionally burdensome, difficult to fully comply with, and could easily require hundreds of thousands, if not millions, of dollars in compliance costs. For those reasons, Neustar's proposed requirement would violate the PRA.

A login requirement's violation of the PRA is underscored by the fact that mechanisms are already in place to address waste, fraud or abuse concerns. Sorenson already requires all users who place a VRS call from a public phone to digitally sign a self-certification indicating that they are deaf or hard-of-hearing and need VRS in order to communicate, preventing any inadvertent misuse of the phone. Moreover, because Deaf and hard-of-hearing persons are eligible and entitled to use VRS, so long as the person is Deaf or hard-of-hearing, there is no issue of ineligible use. Besides, unlike IP Relay, which allows complete anonymity for users that may or may not use ASL, VRS requires the user to appear on video and communicate with a communications assistant ("CA") in ASL during each call. CAs are required to terminate any call that does not involve an individual that uses ASL or that otherwise does not appear to be a legitimate VRS call.

* * *

Neither the *FNPRM* nor the record supports Neustar's proposal for a login requirement using OAuth. Such a requirement would violate functional equivalence by subjecting Deaf persons to burdens not faced by hearing individuals, and would be arbitrary and capricious because it would impose substantial burdens on both Deaf VRS users and VRS providers without even meager offsetting benefits. Moreover, such a requirement could not possibly pass OMB review under the PRA. Accordingly, Sorenson urges the Commission to reject Neustar's proposal.

Sincerely,

John T. Nakahata
Counsel to Sorenson Communications, LLC